

## Pearson BTEC Level 3 Nationals Diploma, Extended Diploma

**Window for supervised period:**

**Monday 6 January 2020 – Friday 24 January 2020**

Supervised hours: 5 hours

Paper Reference **20158K**

# Information Technology

## Unit 11: Cyber Security and Incident Management

**Part A**

### You will need:

Risk\_Assessment.rtf

Security\_Plan.rtf

### Instructions

- **Part A** and **Part B** contain material for the completion of the set tasks under supervised conditions.
- There are 43 marks for **Part A** and 37 marks for **Part B**, giving a total mark for the set task of 80.
- **Part A** and **Part B** are specific to each series and this material must be issued only to learners who have been entered to take the tasks in the specified series.
- This booklet should be kept securely until the start of the 5-hour, **Part A** supervised assessment period.
- **Part A** will need to have been completed and kept securely before starting **Part B**.
- Both parts will need to be completed during the 3-week period timetabled by Pearson.
- **Part A** and **Part B** tasks must be submitted together for each learner.
- This booklet should not be returned to Pearson.
- Answer **all** activities.

### Information

- The total mark for this paper is 43.

Turn over ►

R64088A

©2020 Pearson Education Ltd.

1/1/1/1



Pearson

## Instructions to Invigilators

This paper must be read in conjunction with the unit information in the specification and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document. See the Pearson website for details.

Refer carefully to the instructions in this task booklet and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document to ensure that the assessment is supervised correctly.

**Part A** and **Part B** set tasks should be completed during the period of 3 weeks timetabled by Pearson. **Part A** must be completed before starting **Part B**.

The 5-hour, **Part A** set task must be carried out under supervised conditions.

The set task can be undertaken in more than one supervised session.

Electronic templates for activities 1 and 2 are available on the website for centres to download for learner use.

Learners must complete this task on a computer using the templates provided and appropriate software. All work must be saved as PDF documents for submission.

Invigilators may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Invigilators should note that they are responsible for maintaining security and for reporting issues to Pearson.

### Maintaining Security

- Learners must not bring anything into the supervised environment or take anything out.
- Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.
- Internet access is not permitted.
- Learner's work must be regularly backed up. Learners should save their work to their folder using the naming instructions indicated in each activity.
- During any permitted break, and at the end of the session, materials must be kept securely and no items removed from the supervised environment.
- Learners can only access their work under supervision.
- User areas must only be accessible to the individual learners and to named members of staff.
- Any materials being used by learners must be collected in at the end of each session, stored securely and handed back at the beginning of the next session.
- Following completion of **Part A** of the set task, all materials must be retained securely for submission to Pearson.
- **Part A** materials must not be accessed during the completion of **Part B**.

## Outcomes for Submission

Each learner must create a folder to submit their work. Each folder should be named according to this naming convention:

**[Centre #]\_[Registration number #]\_[surname]\_[first letter of first name]\_U11A**

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345\_F180542\_Smith\_J\_U11A

Each learner will need to submit 3 PDF documents, within their folder, using the file names listed.

**Activity 1:** activity1\_riskassessment\_[Registration number #]\_[surname]\_[first letter of first name]

**Activity 2:** activity2\_securityplan\_[Registration number #]\_[surname]\_[first letter of first name]

**Activity 3:** activity3\_managementreport\_[Registration number #]\_[surname]\_[first letter of first name]

An authentication sheet must be completed by each learner and submitted with the final outcomes.

The work should be submitted no later than 28 January 2020.

## Instructions for Learners

Read the set task brief carefully.

Plan your time carefully to allow for the preparation and completion of all the activities.

Your centre will advise you of the timing for the supervised period. It is likely that you will be given more than one timetabled session to complete these tasks.

Internet access is not allowed.

You will complete this set task under supervision and your work will be kept securely at all times.

You must work independently throughout the supervised assessment period and must not share your work with other learners.

Your invigilator may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

You should only consider threats, vulnerabilities, risks and security protection measures that are implied and/or specified in the set task brief.

**Part A** materials must not be accessed during the completion of **Part B**.

### Outcomes for Submission

You must create a folder to submit your work. Each folder should be named according to this naming convention:

**[Centre #]\_[Registration number #]\_[surname]\_[first letter of first name]\_U11A**

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345\_F180542\_Smith\_J\_U11A

You will need to submit 3 PDF documents within your folder, using the file names listed.

**Activity 1:** activity1\_riskassessment\_[Registration number #]\_[surname]\_[first letter of first name]

**Activity 2:** activity2\_securityplan\_[Registration number #]\_[surname]\_[first letter of first name]

**Activity 3:** activity3\_managementreport\_[Registration number #]\_[surname]\_[first letter of first name]

You must complete an authentication sheet before you hand your work to your invigilator.

## Set Task Brief

### Brilliant Billboards

Ben Jacobson owns Brilliant Billboards (BB). It is a small but rapidly expanding business that supplies digital information services for events. Ben considers BB to be a modern version of traditional paper-based posters and advertising billboards. BB is based in a small industrial unit in Milton Keynes. Ben also works from his home office in the nearby town of Bletchley.

For each event BB provides a network of display, control, and communications equipment to meet the needs of the client. This equipment includes devices such as:

- flat display screens and video walls
- touch screen information points
- digital projectors and screens
- wireless access points
- remote access links
- a local server and network infrastructure.

The material displayed at the event can be controlled by four methods.

1. Through the local server, situated at the event location and connected to the event LAN.
2. Via remote access to the local server from BB, using an app written by BB.
3. Through local wireless access by personal devices, using Wi-Fi and/or Bluetooth, depending on the device being used.
4. By keyboard / keypad access to some of the display devices.

Ben wants to expand BB by using this technology in a different situation. Ben has noticed that a lot of poster-type advertising is placed in roadside fields, on temporary sites such as old lorry trailers or piles of hay bales. He has realised that the adverts are only visible during the daytime, so must be placed where there is a lot of natural light.

Ben has developed a prototype system that uses digital display technology to allow adverts to be shown 24/7 and in places where it is too dark to see a poster.

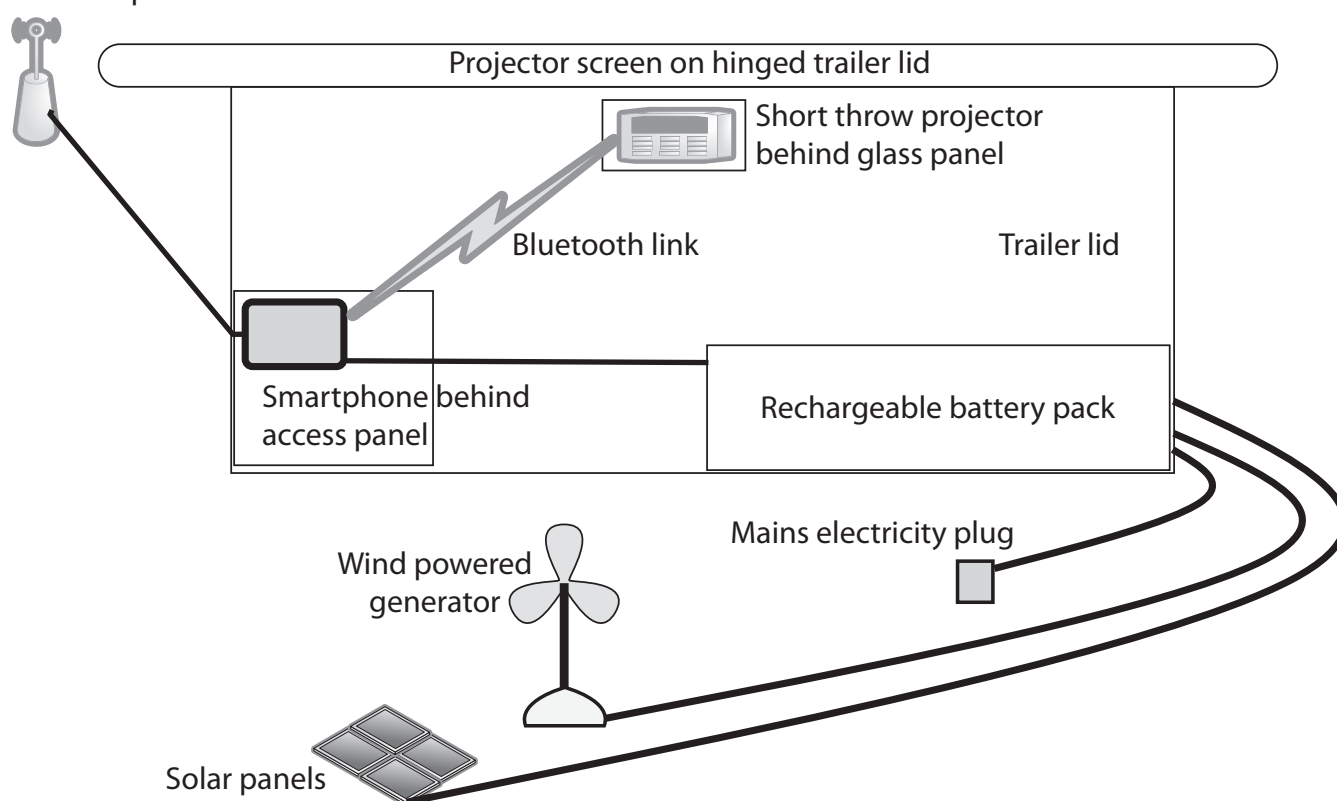
Ben's system uses a trailer that can be set up at advertising sites and then operated locally or remotely in a similar way to the event systems. Each trailer will have a standard set of equipment.

The trailer's equipment is controlled by bespoke software installed on an Android-based smartphone. The smartphone can be accessed by a mobile phone signal, WiFi, or via its touchscreen. The smartphone uses an antenna extension that allows the antenna to be up to ten metres away. The smartphone is placed behind an access panel in the trailer lid. The lid is made of a tough plastic and can be locked. Ben has used old car door locks, which are operated remotely with a radio-frequency identification (RFID) key fob, to secure the lid.

A short throw projector is controlled by the smartphone using Bluetooth. A toughened glass panel is set into the trailer lid to allow the projector to show an image on the screen. The projector screen is connected to the trailer by hinges and folds down when the trailer is moving.

The trailer also contains a rechargeable battery pack, charging leads, solar panels and a wind-powered generator. The panels and generator can be placed up to 100 metres from the trailer if required. **Figure 1** is a plan view of a trailer as it might be set up at an advertising site.

WiFi and phone antenna on extension cable



**Figure 1**

Ben had some concerns about being able to connect to the smartphone when it was in position at a site. He conducted some tests to find out what was possible. His results are shown in **Table 1**.

| Connection distances from Ben's tests |          |  |
|---------------------------------------|----------|--|
| Connection type                       | Distance | Description  |
| Bluetooth to smartphone               | 10 m     | To smartphone, with trailer lid open                   |
| Bluetooth to smartphone               | 2 m      | To smartphone, lid closed, access panel open           |
| Bluetooth to smartphone               | None     | To smartphone, lid and access panel closed             |
| WiFi to smartphone                    | 5 m      | To smartphone, lid and access panel closed             |
| WiFi to smartphone                    | 100 m    | To smartphone via antenna, lid and access panel closed |
| Mobile phone signal to smartphone     | <5 km    | To smartphone, lid and access panel closed             |
| Mobile phone signal to smartphone     | >40 km   | To smartphone via antenna, lid and access panel closed |

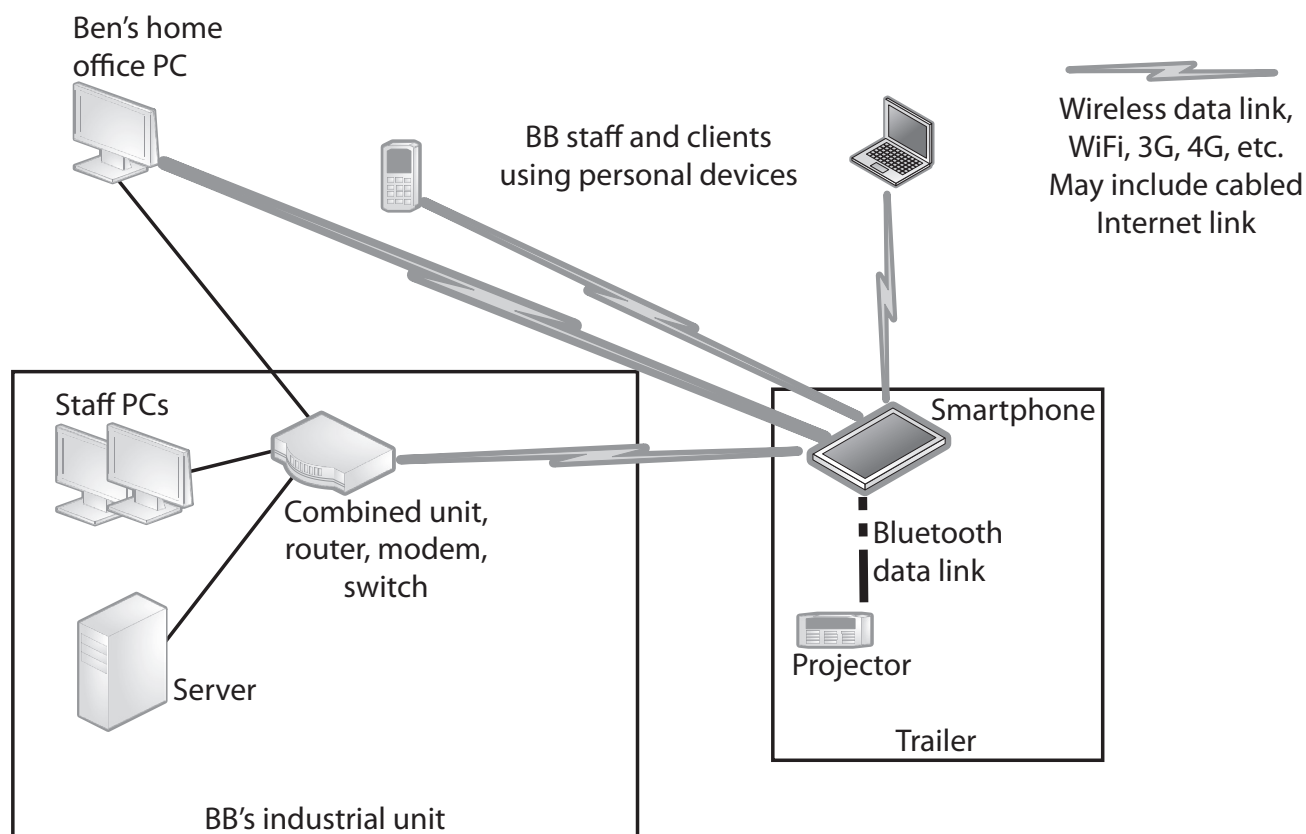
**Table 1**

Ben has more than five years' experience in setting up and securing digital information services for events. He thinks that it is a good idea to have someone, who does not work for BB, to review the trailers. Ben has hired you to advise on cyber security and incident management.

## Development plan

At a meeting with Ben you establish that:

1. Each trailer will conform to the schematic diagram, **Figure 1**.
2. The equipment's connectivity should conform to the network diagram, **Figure 2**, although not all connection methods may be possible at all sites.
3. Ben is concerned about the vulnerability of extension cables.
4. Ben wants to use the same app that he uses for the local servers at events to give access to the smartphones in the trailers.
5. Ben wants to standardise the lid locks for all the trailers.
6. Ben is concerned about the security implications of using WiFi and mobile phone signals.
7. It must be easy to change what the projector is showing.
8. Both BB and advertising clients should be able to connect using the BB app with personal devices.
9. Clients should only be able to connect to smartphones that are controlling the display of their own adverts.
10. Clients who can connect to smartphones should only be able to alter their own adverts.
11. A failure in a smartphone or Bluetooth link should not stop adverts from being displayed.



**Figure 2**

## Part A Set Task

**You must complete ALL activities in the set task.**

**Read the set task brief carefully before you begin and note that reading time is included in the overall assessment time.**

You should only consider threats, vulnerabilities, risks and protection measures that are implied and/or specified in the set task brief.

Design cyber security protection measures for the given computer network.

### **Activity 1: Risk assessment of the networked system**

Duplicate (copy and paste) and complete the risk assessment using the template given for each threat.

Produce a cyber security risk assessment using the template **Risk\_Assessment.rtf**

Save your completed risk assessment as a PDF in your folder for submission as **activity1\_riskassessment\_[Registration number #]\_[surname]\_[first letter of first name]**

You are advised to spend 1 hour and 30 minutes on this activity.

---

**(Total for Activity 1 = 8 marks)**

### **Activity 2: Cyber security plan for the networked system**

Using the template **Security\_Plan.rtf** produce a cyber security plan for the computer network using the results of the risk assessment.

For each protection measure, you must consider:

- (a) threat(s) addressed by the protection measure
- (b) action(s) to be taken
- (c) reasons for the action(s)
- (d) overview of constraints – technical and financial
- (e) overview of legal responsibilities
- (f) overview of usability of the system
- (g) outline cost-benefit
- (h) test plan.

Duplicate (copy and paste) and complete the cyber security plan using the template given for each protection measure, as appropriate.

Save your completed security plan as a PDF in your folder for submission as **activity2\_securityplan\_[Registration number #]\_[surname]\_[first letter of first name]**

You are advised to spend 2 hours and 30 minutes on this activity.

---

**(Total for Activity 2 = 20 marks)**



### Activity 3: Management report justifying the solution

Produce a management report, justifying how the proposed cyber security plan will meet the security requirements of the set task brief.

The report should include:

- an assessment of the appropriateness of your protection measures
- a consideration of alternative protection measures that could be used
- a rationale for choosing your protection measures over the alternatives.

Save your completed management report as a PDF in your folder for submission as **activity3\_managementreport\_[Registration number #]\_[surname]\_[first letter of first name]**

You are advised to spend 1 hour on this activity.

---

**(Total for Activity 3 = 12 marks)**

---

**TOTAL FOR TECHNICAL LANGUAGE IN PART A = 3 MARKS**

**TOTAL FOR PART A = 43 MARKS**